DIGITALE TRANSFORMATION MUSS SECURITY EINBEZIEHEN

WHITEPAPER

Unternehmen stellen sich um, um auf dem neuen digitalen Markt effektiver konkurrieren zu können. Neue Datenanforderungen machen es zwingend erforderlich, dass Unternehmensnetzwerke schneller und effizienter laufen. Daten werden aus einer Vielzahl von Quellen erfasst, einschließlich neuer IoT-Geräte mit verschlüsselten Daten, und werden dann verarbeitet, um wertvolle und wettbewerbsfähige Informationen zu gewinnen und bereitzustellen – die Grundlage der neuen digitalen Wirtschaft, der Digital Economy.

Es überrascht nicht, dass herkömmliche Netzwerkarchitekturen – aufgebaut auf veralteten Netzwerkgeräten, die im Laufe der Jahre von Dutzenden verschiedenen Anbietern erworben wurden – nicht dafür ausgelegt sind, die modernen Anforderungen hinsichtlich Leistung, Flexibilität und Effizienz zu erfüllen. Die meisten Unternehmen implementierten ursprünglich Lösungen von Dutzenden von Anbietern, um einzelne Schwachstellen zu vermeiden. Ein solcher Ansatz schwächt jedoch ihr Sicherheitsprofil, da er die Fähigkeit, Bedrohungen zueinander in Beziehung zu setzen, verringert und gleichzeitig den Management-Aufwand steigert.

In den vergangenen Jahren haben Unternehmen daher ihre Netzwerk-Hardware rasch durch virtuelle Server und cloudbasierte Infrastruktur ersetzt und die Anzahl der Anbieter, mit denen sie arbeiten, verringert. Dieser Konsolidierungsprozess sorgt nicht nur für IT- und Rechenzentrumseffizienz, sondern senkt auch die laufenden Investitions- und Betriebskosten. Weniger Geräte von weniger Anbietern bedeutet, dass begrenzte IT-Ressourcen sich wieder auf das Kerngeschäft des Unternehmens konzentrieren können. Die Anbieterkonsolidierung verringert auch die Anzahl der zu überwachenden Management-Konsolen, verbessert Sichtbarkeit und Kontrolle und ermöglicht einen höheren Grad der Automatisierung.

Immer mehr Geräte am Netzwerkrand wechseln in die Cloud und das Netzwerk wird immer verteilter und transienter. Demzufolge müssen auch die herkömmlichen perimeterbasierten Sicherheitsstrategien geändert werden. Während der Netzwerk-Overhead reduziert wird, nimmt die Zahl der Sicherheitsgeräte in den Netzwerken zu.

Diese Zunahme von Sicherheitsgeräten und -anbietern in den Unternehmen hat zwei Ursachen.

Zum einen ist das Netzwerk selbst trotz der abnehmenden Zahl von Anbietern und physischen Geräten, die verwaltet werden müssen, komplexer geworden. Daten und Ressourcen sind auf eine Vielzahl von Domains, einschließlich Public und Private Clouds, mobile Endgeräte und entfernte Standorte, verteilt, und die Netzwerke selbst sind nicht mehr statisch. Für herkömmliche Security Tools wird es immer schwieriger, dynamische, reaktionsfähige und zunehmend transiente Netzwerke zu verfolgen – von der Prüfung und Sicherung der wachsenden Zahl von Daten, Geräten und Benutzern in diesen Netzwerken ganz zu schweigen.

Zum anderen ändert sich auch das Wesen der Cyber-Kriminalität. Angriffe, wie der derzeitige Anstieg von Ransomware, werden sowohl komplexer als auch teurer. Zudem setzen neue mehrstufige Angriffe nicht nur selbstlernende und ausgeklügelte Verschleierungstechniken ein, sondern zielen gleichzeitig über das verteilte Netzwerk hinweg auf eine Vielzahl von Angriffsvektoren ab, wie etwa die große Zahl von Endgeräten und Cloud-Umgebungen. Sie nutzen auch die Einschränkungen vieler bestehender Security-Implementierungen, indem Sie sich lateral durch ein Unternehmen bewegen, um nicht erkannt zu werden.

Um diesen Herausforderungen zu begegnen, kaufen und implementieren Unternehmen spezialisierte Sicherheitsinstrumente, sowohl um neuen Bedrohungen entgegenzutreten als auch um in neuen Umgebungen zu arbeiten und Dinge wie Hypervisor, Cloud-Umgebungen, Zugangspunkte und Endgeräte zu unterstützen. Diese Lösungen sind jedoch häufig einfach mehr von der gleichen Medizin – isolierte Geräte, deren Implementierung, Abstimmung und Verwaltung zusätzliche Ressourcen erfordert.

Die daraus entstehenden Herausforderungen sind vorhersehbar.

- **Höherer IT-Overhead** – Security-Geräte müssen eingerichtet, aktualisiert und verwaltet werden. Netzwerkumgebungen ändern sich automatisch, um der Verlagerung des Datenverkehrs, dem Datenvolumen und den Anforderungen des Datenverkehrs gerecht zu werden. Um diesen sich verändernden Netzwerkparadigmen zu

begegnen, müssen die Sicherheitsregeln aktualisiert und geändert werden. Das alles kann nicht mehr manuell erledigt werden. Für jedes neue Tool ist ein Techniker erforderlich, der mit der Konfiguration und dem Betriebssystem vertraut ist, das Tool für das zu schützende Netzwerksegment einrichten und seine Sicherheits- und Bedrohungsdaten auf dem neuesten Stand halten kann. Hierfür ist häufig mehr Personal erforderlich, als es sich die meisten Unternehmen leisten können. Sicherheits-Tools laufen daher oft mit suboptimaler Effizienz, Teile der Daten- und Netzwerksegmente sind häufig nur unzureichend abgesichert und unregelmäßige und unvorhersehbare Update-Zyklen führen dazu, dass Geräte anfällig oder weniger effektiv sind.

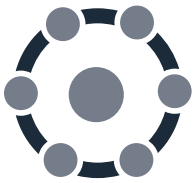
- **Komplexes Management** – Jede Security-Lösungsfamilie hat gewöhnlich eine eigene Verwaltungskonsole, die nur eine Sicht auf die Tools und die Daten bereitstellt, die sie kontrollieren soll. Bei einem Dutzend oder mehr Anbietern von Sicherheitslösungen führt dies zu einem logistischen Verwaltungsalbtraum. Das Ganze wird zusätzlich dadurch erschwert, dass diese Geräte nicht für das Teilen von Bedrohungsdaten konzipiert sind. IT-Teams sind daher gezwungen, Informationen manuell zueinander in Beziehung zu setzen, um moderne, komplexe Bedrohungen zu erkennen. Das bedeutet, dass der Zeitraum von der Infizierung eines Netzwerks bis zur Erkennung der Bedrohung häufig Wochen beträgt, anstelle von Minuten oder Sekunden, die tatsächlich nur zur Verfügung stehen, um das Betriebsvermögen effektiv zu verteidigen.
- **Isolierte Geräte können nicht als System reagieren** – Wenn ein Angriff erkannt wurde, müssen Sie ermitteln, woher er kam, wie lange er schon andauert, welche Geräte betroffen sind und wie er beseitigt werden kann. Das bedeutet, Ihre Sicherheitslösung muss in der Lage sein, für jede erkannte Bedrohung eine koordinierte Reaktion zu synchronisieren. Isolierte Geräte sind dazu leider nicht fähig und bestimmte Segmente des Netzwerks können daher leicht übersehen werden. Viel zu oft bleiben Private oder Public Cloud-Umgebungen in puncto Sicherheit ein blinder Fleck.
- **Kompetenzlücke im Bereich Security** – Schlimmer noch, all dies geschieht zu einem Zeitpunkt, zu dem erfahrene Spezialisten, die die erforderlichen Security-Schulungen und -Fähigkeiten mitbringen, immer schwerer zu finden sind. Experten schätzen, dass es derzeit weltweit eine Million unbesetzte Stellen für den Bereich Cyber-Sicherheit gibt, und diese Zahl bis 2019 auf 1,5 Millionen anwachsen wird.

LAYERING AUTOMATISIERTER SICHERHEITSMECHANISMEN

Wie die Netzwerke, die geschützt werden sollen, müssen auch die Sicherheitsmechanismen neu durchdacht und mit umgestellt werden. Um moderne dynamische Netzwerke zu unterstützen, müssen Sicherheitslösungen jedes einzelne Gerät im Netzwerk sehen, Richtlinien am Access Point einrichten und Daten und Ressourcen über die gesamte verteilte Umgebung hinweg überwachen und schützen: vom IoT, über das Netzwerk bis in die Cloud. Hierzu ist ein architektonischer oder Fabric-basierter Sicherheitsansatz erforderlich, der übergreifende Integration, nahtlose Zusammenarbeit und automatisierte Anpassbarkeit ermöglicht.

Um dies zu erreichen, müssen Sie beginnen, Ihre veralteten und isolierten Security-Geräte und -Plattformen durch Tools zu ersetzen, die darauf ausgelegt sind, entweder unter einem gemeinsamen Betriebssystem oder durch die Einhaltung gemeinsamer Standards zusammenzuarbeiten. Wenn möglich, wechseln Sie zu einem einzigen Anbieter, der eine einheitliche Verwaltung und Kontrolle der Lösungen, die an physischen, virtuellen oder dezentralen Standorten oder in der Cloud bereitgestellt werden, ermöglicht, und somit eine einheitliche Orchestrierung und Durchsetzung der Richtlinien. Wenn dies nicht möglich ist, sollte nach Lösungen gesucht werden, die offene Standards unterstützen und nahtlos in das Security- und Management-Framework integriert werden können.

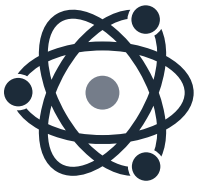
Tools, die in eine ganzheitliche Security Fabric eingebunden werden können, bieten stets bessere Sichtbarkeit und Kontrolle als solche, die isoliert arbeiten. Sie können aktiv Bedrohungsdaten sammeln und weitergeben, um Sichtbarkeit und Intelligenz zu verbessern, Situationsbewusstseint zu erhöhen und eine synchronisierte Angriffsreaktion überall im Netzwerk möglich zu machen. Dieser Ansatz erlaubt es Unternehmen, drei grundlegende Sicherheitsanforderungen von modernen Netzwerken zu erfüllen:



UMFASSENDE ABDECKUNG

Eine effektive Sicherheitsimplementierung muss die gesamte Angriffsfläche abdecken und in Echtzeit auf erkannte Bedrohungen und dynamische Änderungen innerhalb des Netzwerks reagieren. Netzwerkadministratoren müssen Einblick in die gesamte Umgebung haben, einschließlich Endgeräte, Access Points, IoT-Geräte, Netzwerkelemente, Rechenzentrum, Cloud und sogar Anwendungen und Daten selbst.

Eine einheitliche Sicht über das erweiterte und zunehmend elastische Unternehmen hinweg kann nicht um isolierte Geräte herum bereitgestellt werden. Ein Sicherheits-Framework basierend auf offenen Standards ermöglicht es Lösungen, als einheitliches System zu arbeiten. Ein solcher Ansatz hilft Administratoren, Daten, Anwendungen, Geräte und Arbeitsabläufe miteinander zu verbinden, um über das verteilte Unternehmen hinweg die komplexesten Bedrohungen zu finden und sie abzuwehren.



INTEGRATION

Zahlreiche der modernen und besonders komplexen Bedrohungen sind so konzipiert, dass sie einer Erkennung entgehen. Sie umgehen Edge Security Gateways, indem sie sich in verschlüsseltem Datenverkehr verbergen, mehrstufige Angriffe verwenden, die zunächst harmlos aussehen und Benutzer dazu veranlassen, ein Schadprogramm herunterzuladen und auszuführen, oder indem sie durch ein infiziertes Gerät direkt in das Netzwerk gelangen. Wenn sie einmal einen Weg in das Netzwerk gefunden haben, beobachten sie legitime Netzwerk-Datenverkehrsmuster und ahmen sie nach, um sich im Netzwerk auszubreiten. Sie können auch für lange Zeiträume „schlummern“ und auf einen Befehl oder bestimmte Umstände warten, durch die sie aktiviert werden. Aus diesen Gründen kann ein erfolgreiches Eindringen in einem infizierten Netzwerk über Wochen oder Monate, in denen sensible Daten gesammelt und abgegriffen werden können, unentdeckt bleiben.

Einer der Faktoren, die zu dieser Herausforderung beitragen, ist, dass viele der Security Tools, die Unternehmen über ihre Netzwerke hinweg einsetzen, isoliert arbeiten. Sie sehen nur den Datenverkehr, der direkt vor ihnen übertragen wird, und können keine Bedrohungsdaten teilen oder zueinander in Beziehung setzen, um ein größeres Bild zu erhalten. Dies ist jedoch erforderlich, um diese komplexen Bedrohungen zu erkennen.

Dieses Problem ist besonders gravierend, wenn Daten und Workloads zwischen herkömmlichen und Multi Cloud Domains übertragen werden. Viel zu oft sind Sicherheitsspezialisten gezwungen, Logs auf separaten Konsolen zu prüfen und Daten manuell zueinander in Beziehung zu setzen, um komplexe Bedrohungen zu erkennen. Bei durchschnittlich

mehr als 30 Einzelprodukten in einem typischen Unternehmensnetzwerk sind die damit verbundenen Herausforderungen jedoch von den verfügbaren Ressourcen der meisten IT-Teams nicht zu schultern.

Was Unternehmen brauchen, sind Security-Geräte, die darauf ausgelegt sind, Bedrohungen zu erkennen, weiterzugeben, in Beziehung zu setzen und auf sie zu reagieren. Das bedeutet, dass Security Tools nicht nur basierend auf ihrer Leistung und ihren Funktionen gewählt werden müssen, sondern auch anhand ihrer Fähigkeit, als Teil eines integrierten Security-Systems zu arbeiten. Sie müssen daher ein gemeinsames Betriebssystem verwenden oder über offene Standards einbeziehbar sein. Sie müssen außerdem fähig sein, innerhalb eines zentralisierten Analyse- und Management-Systems zu arbeiten, das Daten zueinander in Beziehung setzen und eine automatisierte Abwehrreaktion auf eine erkannte Bedrohung orchestrieren kann. Sicherheitsmechanismen, die um ein Framework integrierter Geräte herum konzipiert sind ermöglichen eine einfachere Erkennung von komplexen Verhaltensweisen und Mustern von Bedrohungen. Infizierte Geräte oder Netzwerksegmente können dynamisch isoliert und beseitigt und schädliche Malware kann entlang der Angriffskette bis zu ihrem Ausgangspunkt zurückverfolgt werden. Verteilte Security Tools können somit als System arbeiten und kontinuierlich Gefahrenbewertungen über die gesamte verteilte Netzwerkumgebung hinweg liefern.

AUTOMATISIERUNG

Da ein Angriff ein Netzwerk innerhalb weniger Minuten infizieren kann, ist Sichtbarkeit alleine nicht ausreichend. Eine integrierte Sicherheitsarchitektur, die Security-Lösungen zu einer holistischen Lösung verbindet, gestattet es, schnell und koordiniert auf Bedrohungen zu reagieren. Sicherheitselemente können nicht nur schnell lokale und globale Bedrohungsdaten austauschen, sondern auch automatisch eine koordinierte Abwehrreaktion koordinieren. So können infizierte Geräte isoliert und entfernt, Richtlinien aktualisiert, ähnliche Gefahrensituationen gesucht, Netzwerksegmente und Access Points automatisch gesichert, Indicators of Compromise erhöht und Malware beseitigt werden.

In modernen elastischen Netzwerkumgebungen müssen Sicherheitslösungen sich automatisch an sich ändernde Netzwerkkonfigurationen anpassen. Wenn sich das geschützte Netzwerk aufgrund sich ändernder Geschäftsanforderungen wandelt, müssen neue Richtlinien eingerichtet und durchgesetzt werden. Gleichzeitig müssen zusätzliche Sicherheitsmaßnahmen und Gegenmaßnahmen aktualisiert oder automatisch bereitgestellt werden, wenn neue Geräte, Workloads und Dienste implementiert werden. Hierbei müssen auch automatisierte Auditing- und Sicherheitsanpassungen einbezogen werden, damit auch innerhalb des geänderten Netzwerks Compliance gewährleistet ist.

VORTEILE EINER SECURITY FABRIC

Die Vorteile der Konsolidierung Ihrer Sicherheitslandschaft sind ähnlich jenen, die Sie durch die Konsolidierung Ihrer Netzwerk-Ressourcen erhalten: niedrigere Investitions- und Betriebskosten, größere Sichtbarkeit und Kontrolle, weniger Implementierungen von Security Tools, schnellere Notfallwiederherstellung sowie einfachere und skalierbare Compliance mit gesetzlichen Anforderungen.

Die Fortinet Security Fabric ist das erste Framework, das einen umfassenden architektonischen Security-Ansatz bereitstellt. Sie können verteilte Sicherheitslösungen in einem einheitlichen Framework verbinden, das sich dynamisch an Ihre sich ändernde IT-Infrastruktur anpasst und die sich schnell ändernde und zunehmend verteilte Angriffsfläche verteidigt. Der auf offenen Standards aufbauende Ansatz erlaubt es Ihnen, Software und Lösungen einer Vielzahl von Anbietern zu integrieren, um so nahtlosen Schutz und verwertbare Bedrohungsdaten über alle Punkte Ihres Netzwerks hinweg, vom IoT-Gerät bis zur Cloud, bereitzustellen.

FORTINET

DEUTSCHLAND
Feldbergstraße 35
60323 Frankfurt
Deutschland
Telefon: +49 69 310 192 0

SCHWEIZ
Riedmuehlestr. 8
CH-8305 Dietlikon/Zürich
Schweiz
Telefon: +41 44 833 68 48

ÖSTERREICH
Wienerbergstrasse 11
Turm A
9.OG, 1100 Wien
Österreich
Verkaufsabteilung:
Telefon: +43 1 3760013 - 0

HAUPTSITZ
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
USA
Tel.: +1 408 235 7700
www.fortinet.com/sales

VERTRIEBSBÜRO
EMEA
905 rue Albert Einstein
06560 Valbonne
Frankreich
Tel.: +33 4 8987 0500

VERTRIEBSBÜRO
APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel.: +65 6513 3730

LATEINAMERIKA
ZENTRALE
Sawgrass Lakes Center
13450 W. Sunrise Blvd.,
Suite 430
Sunrise, FL 33323
Tel: +1 954 368 9990

90833 0 0 EN
Juli 13, 2018 10:26 vorm.